PATENT 7251/94672

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Belenky et al.

For: IMPROVED CFM MODE SYSTEM

Serial No.: 10/541,002

371 Submission of: PCT/IL2004/000144
filed 16 FEB 2004

INFORMATION DISCLOSURE STATEMENT

Mail Stop PCT Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450

Sir or Madam:

In accordance with 37 C.F.R. §§1.56, 1.97 and 1.98, applicants submit a list of documents, general remarks, an attached Form PTO-1449, and copies of the documents except for the U.S. patents.

U.S. Patent No.	<u>Date of Issue</u>	Inventor
4,229,818	21 OCT 1980	Matyas et al.
4,731,843	15 MAR 1988	Holmquist
6,249,582	19 JUN 2001	Gilley
6,578,150	10 JUN 2003	Luyster

Foreign Patent Pub.	Date of Publication	Country
WO 99/66669	23 DEC 1999	PCT
EP 0 996 250 A2	26 APR 2000	EP

Other Documents

D. Eastlake et al., "US Secure Hash Algorithm 1 (SHA1)" (Network Working Group, Request for Comments 3174, September 2001) (available on World Wide Web at http://www.ietf.org/rfc/rfc3174.txt?number=3174).

"Advanced Encryption Standard (AES)" (Federal Information Processing Standards Publication 197, 26 November 2001).

"DES Modes of Operation" (Federal Information Processing Standards Publication 81, 2 December 1980) (available on World Wide Web at http://csrc.nist.gov/publications/fips/fips81/fips81.htm).

"Secure Hash Standard" (Federal Information Processing Standards Publication 180-1, 17 April 1995) (available on World Wide Web at http://www.itl.nist.gov/fipspubs/fip180-1.htm).

"What is Cipher Feedback Mode?" (RSA Security, Inc. 2003) (available on World Wide Web at http://www.rsasecurity.com/rsalabs/faq/2-1-4-4.html).

It is requested that each of the above documents be given consideration by the Examiner and made of record in the captioned patent application. The International Search Report is also attached.

Respectfully submitted,

L. Friedman
Req. No. 37,135

28 September 2005

WESLH & KATZ, LTD. 120 South Riverside Plaza 22nd Floor Chicago, Illinois 60606 (312) 655-1500 Docket Number (Optional)

7251/9462

Application Number

10/541,002

Applicant(s)

Belenk, et al.

Filing Date 371 Submission of: Court April 18

PCT/IL2004/000144 filed 16 FEB 2004 **U.S. PATENT DOCUMENTS** EXAMINER FILING DATE CLASS SUBCLASS REF DOCUMENT NUMBER DATE NAME INITIAL IF APPROPRIATE 21/10/1980 4,229,818 Matyas, et al. 15/03/1988 Holmquist 4,731,843 6,249,582 19/06/2001 Gilley 10/06/2003 6,578,150 Luyster U.S. PATENT APPLICATION PUBLICATIONS *EXAMINER FILING DATE CLASS SUBCLASS DATE NAME DOCUMENT NUMBER REF INITIAL IF APPROPRIATE FOREIGN PATENT DOCUMENTS Translation SUBCLASS COUNTRY CLASS REF DOCUMENT NUMBER DATE YES NO 23/12/1999 **PCT** WO 99/66669 EP 0 996 250 A2 26/04/2000 EP (Including Author, Title, Date, Pertinent Pages, Etc.) OTHER DOCUMENTS D. Eastlake, et al., "US Secure Hash Algorithm 1 (SHA1)" (Network Working Group, Request for Comments 3174, September 2001) (available on World Wide Web at http:///www.ietf.org/rfc/rfc3174.txt?number=3174). "Advanced Encryption Standard (AES)" (Federal Information Processing Standards Publication 197,26 November 2001) DATE CONSIDERED **EXAMINER**

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Docket Number (Optional) 7251/94622 Application Number

10/541,002

Applicant(s)

Belen., et al.

U.S. PATENT DOCUMENTS									
*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE		NAME	CLASS	SUBCLASS	FILING IF APPRO	
		_							
			U.S. PATENT	Γ APPLICA	TION PUBLICATIONS				
*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE		NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
•									
			FORE	IGN PATEN	T DOCUMENTS				
ï	REF	DOCUMENT NUMBER	DATE		COUNTRY	CLASS	SUBCLASS	Translation YES NO	
		National Control of Co							
									
			OTHER E	OCUMENT	rs (Including Aut	hor, Title, Date, Per	tinent Pages, Ei	(c.)	
		"DES Modes of Ope World Wide Web at htt	ration" (Federal) p://csrc.nist.gov /	Informatio nublication	n Processing Standards is/fips/fips81/fips81.htm	Publication 81, 2 1).	2 December 19	980) (availa	ible on
		"Secure Hash Stand World Wide Web at htt	ard" (Federal In p://www.itl.nist.g	formation l ov/fipspub	Processing Standards P s/fip180-1.htm).	ublication 180-1,	17 April 1995) (availabl	e on
EXAMINE	R				DATE CONSIDERED				
EXAMINE	R: Initia	l if citation considered, whether	or not citation is in	conforman	ce with MPEP Section 609): Draw line throug	h citation if not	in conform	ance and

not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLORE CITATION

(Use several sheets if necessary)

Docket Number (Optional)
7251/9

Application Number

10/541,002

Applicant(s)

Belenky, et al.

Filing Date 371 Submission of: Group AAT Out.
PCT/IL2004/000144 filed 16 FEB 2004

U.S. PATENT DOCUMENTS									
*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING IF APPRO		
			U.S. PATENT	APPLICATION PUBLICATIONS					
*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE		
	-		FORE	IGN PATENT DOCUMENTS					
	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Trans YES	Translation YES NO	
			OTHER D	OCCUMENTS (Including Autho	r, Title, Date, Per	rtinent Pages, Et	c.)		
"What is Cipher Feedback Mode?" (RSA Security, Inc. 2003) (available on World Wide Web at http://www.rsasecurity.com/rsalabs/faq/2-1-4-4.html).									
			-						
EXAMINE	R		,	DATE CONSIDERED					
EXAMINE	R: Initi	al if citation considered, whether	or not citation is in	conformance with MPEP Section 609;	Draw line throug	gh citation if not	in conform	ance and	

Form PTO-A820 (also form PTO-1449)

not considered. Include copy of this form with next communication to applicant.

P09A/REV05

OF 3